PathGetShortPath

The destination string buffer must be long enough to hold the return file path

Sean Barnum, Cigital, Inc. [vita[1]]

2007-04-02

Part "Original Cigital Coding Rule in XML"

Mime-type: text/xml, size: 3876 bytes

Attack Category	• Malicious Input • Path spoofing or confusion problem
Vulnerability Category	• Buffer Overflow • Unconditional
Software Context	• File Path Management
Location	• shellobj.h
Description	The in/out destination string buffer of function PathGetShortPath() must be long enough to hold an expanded file path. The PathGetShortPath() modifies the path parameter, in place, to find the "shortest path name" for the long path specified. A short path is usually defined in 8.3 standards. However, since the input path might be relative, it is possible for the resulting path to be longer that the input path. Therefore, the path variable should be at least MAX_PATH characters in length. This routine is part of a deprecated shellobj.h module that can be replaced with GetShortPathName.
APIs	**Function Name** / **Comments** PathGetShortPath
Method of Attack	This routine modifies a path parameter IN PLACE to convert it to a short path name (8.3 format). However, it is not guaranteed to be shorter than the original path due to relative path expansion. Therefore, the path buffer must provide extra space for expansion. Otherwise, an attacker might be able to provide a path name that expands and overflows the buffer.
Exception Criteria	
Solutions	**Solution Applicability** / **Solution Description** / **Solution Efficacy**

1. http://buildsecurityin.us-cert.gov/bsi-rules/35-BSI.html (Barnum, Sean)

	Whenever PathGetShortPath() is used.	The parameter, pszLongPath, must be at least MAX_PATH characters in length. Consider replacing with GetShortPathName which takes separate in and out buffers.	Effective.
Signature Details	void PathGetShortPath(LPWSTR pszLongPath);		

Examples of Incorrect Code	`WCHAR path[] = L".\\AShort\ \Path"; // Note: buffer is too small`
	`LPWSTR pszLongPath = path;`
	`PathGetShortPath(path);`		

Examples of Corrected Code	`WCHAR path[MAX_PATH] = L".\\AShort \\Path"; // Note: buffer is correctly sized`
	`LPWSTR pszLongPath = path;`
	`PathGetShortPath(path);`		

Source Reference	• http://msdn.microsoft.com/library/default.asp?url=/library/en-us/shellcc/platform/shell/reference/functions/pathgetshortpath.asp[2]		
Recommended Resource			
Discriminant Set	**Operating System**	• Windows	
	Languages	• C • C++	

Cigital, Inc. Copyright

1. mailto:copyright@cigital.com